DRAFT

APPENDIX F

PROCEDURES FOR REQUESTING A JTAV IT ACCOUNT

1. General. JTAV In-Theater (IT) account request procedures are in compliance with various DOD and USCINCPAC directives. The USPACOM Certificate of Clearance and AIS/Network Access (AIS/NA) form will be used for USPACOM theater-wide JTAV IT account requests. The procedures begin with a user being recognized to function in a particular billet in a command and needing JTAV IT capability to support that role.

2. Procedures.

   A. Upon successful completion of the JTAV IT Initial User's Training, the user will complete and forward the AIS/NA form. An example of this form is provided as Enclosure (1) to Addendum A. The AIS/NA form will be provided with each copy of the JTAV IT User Manual. Additional copies of the form can be obtained by contacting the JTAV Help Desk Coordinator or on the USPACOM J4 homepage at www.pacom.mil or www.pacom.smil.mil.
      1) USPACOM guidance for completing the AIS/NA form is at Addendum A.
      2) The JTAV Support Office – Pacific (JSOP) needs additional data placed in the AIS/NA form. These instructions are found in Addendum B. Any questions regarding this procedure should be directed to the JSOP Help Desk at (808) 477-4223 or jtavhelp@hq.pacom.mil.
      3) In addition, the user is required to read and sign the JTAV IT Security Briefing found in Addendum C.

   B. Upon completion, the AIS/NA form and Security Briefing should be faxed or mail to the JSOP Help Desk Coordinator:
      1) FAX number is (808) 477-0921.
      2) Mail should be directed to:
         JTAV Support Office Help Desk Coordinator
         P.O. Box 64020
         United States Pacific Command/J4125
         Camp H.M. Smith, HI 96861-4020

   C. The JSOP Help Desk Coordinator (HDC) will forward the user's AIS/NA form to USCINCPAC J4 POC who will complete Section IV "FM (Functional Manager) or OPR (Office of Primary Responsibility)" Signature and Date block of the AIS/NA form.

   D. JSOP System Administrator (SA) will assign an account to the new user and provide a user password for each account (i.e., SIPRNET, NIPRNET, Web, Client/Server) the user is requesting.
      1) The SA will create the account and assign an initial password.
      2) The HDC will then provide each user's command ISSO with the account information. For SIPRNET accounts, the information will be provided through STUIII, and for NIPRNET account information can be sent via UNCLAS email.
      3) Each command ISSO will then provide users with secure account IDs and passwords.

E. The JSOP Help Desk Coordinator will provide a copy of the completed AIS/NA form to the USCINCPAC J6 POC.
F. The JSOP Help Desk Coordinator will record all pertinent user information in a database and keep a paper copy of each user's AIS/NA form and JTAV IT Security Brief agreement.

3. Any additional forms or JTAV IT user Manuals can be requested through the JSOP Help Desk Coordinator.

FOR OFFICIAL USE ONLY
(When Filled In)

HQ, USCINCPAC CERTIFICATE OF CLEARANCE AND AIS/NETWORK ACCESS

COMPLETE SECTION I, II AND IV THEN FORWARD IN TURN TO J2641 and J6413

SECTION I -- COMPLETED BY REQUESTER

1. JTD Billet # *	2. Name (Last, First, Middle Initial) *	3. SSN *	4. Service *	5. Rank/Grade *

6. Telephone (STU-III if avail.) *	7. Staff Code *	8. Rotation Date *	9. Date of Birth *	10. Place of Birth *	11. Duty Status (active, civilian, contractor, reservist) *

12. For Contractor (include contract number, expiration date and COTR), Reservist or Agency(Company or Command Name and Complete Mailing Address)

13. Terminal Type (UNIX/HP/DOS)	14. IP Address	15. Requester's Signature	16. Date

SECTION II -- COMPLETED BY REQUESTING DIRECTORATE OR AGENCY

1. Request individual be granted the security clearance and access authorizations indicated.

□ 2. Confidential □ 3. Secret □ 4. Top Secret □ 5. SIOP-ESI 5a. Category _____________ □ 6. SCI 6a. Compartments ____________

□ 7. PRP □ 8. CNWDI □ 9. Civilian ID Card □ 10. Courier Card (TS/collateral/SCI) □ 10a. Oahu Only □ 10b. Unlimited

11. Division Chief authorization: I confirm access authorization and "need-to-know" of individual requesting access.

□ 12. DDN □ 13. C2S2 □ 13a. ELCCS □ 13b. SNS □ 13c. SMART □ 14. GCCS □ 14a. AMHS

□ 14b. DARWIN □ 15. GCCS-T □ 16. SIOP □ 17. SCI □ 18. JTAV □ 19. Other___________________

20. Justification: *Your E-Mail Address is:

21. GCCS Role: ____________________ 21a. Project Name: ____________________ 21b. Position: ____________________

22. Request individual be granted access to USCINCPAC spaces at times indicated. NOTE: Default access is access to all USCINCPAC spaces from 0630 - 1730 Monday - Friday. Access to a Sensitive Compartmented Information Facility (SCIF) or SIOP-ESI is granted upon indoctrination. Access to other staff sections after duty hours requires authorization.

22a. Building(s): ____________________ 22b. Time(s): ____________________ 22c. Zone(s): ____________________

*	*	*
23. Division Chief Name and Rank	24. Signature	25. Date

26. AISSO/TASO authorization: I confirm access authorization of individual requesting access.

27. AISSO/TASO Name and Rank	28. Signature	29. Date

SECTION III -- COMPLETED BY COMMAND SECURITY OFFICE

1. Type of Investigation	2. Date Completed	3. Conducted by
5. Clearance (Interim /Final) *	6. Granted by	7. Granted Date

9. CERTIFICATION: This certifies that the above named individual has been cleared for/granted access to classified information and material for the classification level indicated in Section III. This clearance/access is granted IAW existing policy on investigation and clearance of DoD personnel for access to classified information, as established by the Secretary of Defense and implementing directives and regulations.

10. Name of official granting clearance/access	11. Signature	12. Date

Privacy Act Statement

AUTHORITY: 5 U.S.C. 301 Departmental Regulation and EO 9397, 22 Nov 43, Numbering System for Federal Accounting Relating to Individuals. PRINCIPAL PURPOSE: To make positive identification of the individual when authorizing access. ROUTINE USE: To develop and maintain the roster of individuals authorized use of the USCINCPAC Automated Information System (AIS) or Network. DISCLOSURE IS VOLUNTARY: Failure to provide information will result in the individual not being authorized use of USCINCPAC AIS or Network. Disclosure of individual identifiable information from this form to any person or agency not entitled to receive it may constitute a misdemeanor punishable by a fine of $5,000 under 5 U.S.C. 552 (a).

SECTION IV -- COMPLETED BY FUNCTIONAL MANAGER (FM) OR OFFICE OF PRIMARY RESPONSIBILITY (OPR)

1. Applications. FM or OPR has approved permissions to the following applications for named individual.

Application	Permissions (R=read, W=write, E=execute)	OPR	FM or OPR Signature and Date
JOPES – Joint Operation Planning & Execution System		J54	
MAT Medical Analysis Tool		J0713	
JFAST – Joint Flow & Analysis for Transportation		J541	
LOGSAFE – Logistics Sustainment Analysis & Feasibility Estimator		J4	
JEPES – Joint Enginner Planning & Execution System		J432	
S&M/AHQ – Scheduling & Movement/Ad Hoc Query		J542	
IRM – Information Resource Manager (FDBM Only)		J542	
RFM – Reference File Manager		J542	
RDA – Requirement Development Analysis		J542	
PDR / JPDRPT – Pre-Defined Reports/Jopes Pre-Defined Reports		J542	
Information Management Subsystem		J542	
JDISS – Joint Deployable Intelligence Support System		J22	
DODIIS Security		J2648	
DODIIS SYSADMIN – System Administrator		J21 SYS	
SCI DASO		J221	
TARGET/ DCP – Theater Analysis & Replanning Graphical Execution Toolkit		J300	
Focal Point		J3	
GRIS – GCCS Reconnaissance Information System		J314	
EVAC – Evacuation System		J32	
FRAS – Fuled Resource & Allocation System		J343	
SIOP—ESI		J374	
GSORTS – GTCCS Status of Resources and Training System		J38	
SIQS – Sorts Interactive Query System		J38	
GTN – Global Transportation Network		J4	
JTAV – Joint Total Asset Visibility	R W E	J41 JTAV	U, W
AMHS – Automated Message Handling Systm {RELEASE AUTHORITY}		J64	
SYBASE Database Administrator)		J6413	
SECMAN – Security Manager		J6413	
Root		J6413	
SYSADMIN – System Administrator		J642	
Oracle Database Administrator		J6422 J54	
JMCIS – Joint Martime Command Information System		CCIP	

SECTION V -- COMPLETED BY COMPUTER SECURITY PERSONNEL

1. LAN Orientation training. Individual requesting access to AIS/Networks attended mandatory course (Computer Security briefing).

2. ISSO Name and Rank ______________________ 3. Signature ______________________ 4. Date ______________

5. SA:	User Account Name	No.	Account Creation Signature/Date	Account Deletion Signature/Date
DDN				
C2S2				
ELCCS	▨	▨		
SNS	▨	▨		
SMART	▨	▨		
GCCS				
AMHS	▨	▨		
DARWIN	▨	▨		
GCCS-T				
SIOP-ESI				
SCI				
Other				

DRAFT

ADDENDUM A to APPENDIX F

USCINCPAC AUTOMATED INFORMATION SYSTEM ACCESS REQUEST PROCEDURES

Ref: (a) DOD Directive 5200.28, Security Requirements for
Automated Information Systems (AIS), 21 March 1988
(b) USCINCPAC Instruction 5510.10J, U.S. Pacific Command
Information Security Program, 20 March 1992

Encl: (1) Automated Information System (AIS) access request form

1. Purpose. To issue policy and assign responsibilities regarding access to USPACOM Automated Information Systems (AIS)

2. Applicability. This instruction applies to all personnel assigned to USPACOM headquarters, or personnel desiring access to any USPACOM AIS.

3. Policy. References (a) and (b) require confirmation of identity and security clearance information before allowing access to USCINCPAC AIS systems.

4. Responsibilities. Completion of Enclosure (1) involves many USPACOM staff members. Responsibilities are as follows:

   a. **Military Elements and the Civilian Personnel Office** shall provide enclosure (1) to all newly assigned personnel.

   b. **Individual requiring AIS access** shall complete Section I of Enclosure (1) and forward it through the chain of command for review by the appropriate Branch Chief.

   c. **Branch Chiefs** shall complete Section II by indicated what types of AIS access the individual requires for fulfilling job requirements; then forward Enclosure (1) to the Command Security Office.

   d. **Command Security Office Personnel** shall complete section III regarding security clearance confirmation and return Enclosure (1) to the individual requesting AIS access.

   e. **Individual requiring AIS access** shall seek out Functional Managers and Offices of Primary Responsibility based upon Branch Chief access authorizations in section II.

   f. **Functional Managers and Offices of Primary Responsibility** shall complete section IV of enclosure (1); based upon Branch Chief Access authorizations in section II.

   g. **Individual requiring AIS access** shall provide Enclosure (1) to the ADP Security Management Branch upon completion of sections I – IV.

h. **ADP Security Management Branch** shall provide necessary computer security training, create AIS accounts and passwords, as necessary, and then forward pertinent personnel information to LAN operations.

i. **LAN Operations Personnel** shall create necessary AIS accounts and passwords and distribute these accounts and passwords to the appropriate personnel, after completion of required computer security training.

JOSEPH E. DEFRANCISCO
Lieutenant General, USA
Deputy USCINCPAC/Chief of Staff

Distribution: (USCINCPACINST 5605.1L)
List IA1, 16-20, 21 (9)
List IB1, 2
List IIA,B, C

ADDENDUM B to APPENDIX F

JTAV IT ACCOUNT REQUEST PROCEDURES

1. Purpose. The purpose of this document is to augment the USPACOM Automated Information System/Network Access (AIS/NA) form procedures (Addendum A) to provide JTAV unique information on the AIS/NA form.

2. User Procedures.
   a. In Section II, Block 20 (Justification) of the AIS/NA form, print your email address, your command and code, and job title as part of the justification for each request.
   b. In Section IV, Permissions column, print the letter (S) if your connection is through the SIPRNET; (U) if the LAN connection is NIPRNET. For the type of access to the database, print the letter (W) for Web access, and the letter (G) for the GUI "client/server" application access. If you have questions regarding which kind of access you will be provided, please call the JTAV Help Desk Coordinator at 808-477-4223.

3. USPACOM J4 POC is recognized as the Functional Manager or Office of Primary Responsibility.

DRAFT

ADDENDUM C to APPENDIX F

SECURITY BRIEFING FOR JOINT TOTAL ASSET VISIBILITY ACCOUNT ACCESS

1. SCOPE.

This briefing applies to all personnel who has access to the JTAV database servers. This access includes use of the JTAV "client/server" software application that is loaded on each desktop, as well as, direct access to the JTAV server via Web access.

2. GENERAL RULES AND PROCEDURES.

a. The rules herein are in addition to, not in lieu of other laws and regulations governing the use of government computers systems and the handling of government owned data (Classified or Unclassified).

b. The JTAV Unclassified server and application is only authorized to process data at that level. No classified data will be processed on that system.

c. The JTAV Secret server and application is only authorized to process data up to and including the SECRET level. No TOP SECRET, SCI, ORCON, NATO or other caveat information will be processed on that server.

d. Use of the JTAV Servers for other than official business is prohibited.

e. Use of the JTAV Servers constitutes consent to monitoring.

f. JTAV Server users WILL NOT add, delete or modify files on any of the JTAV Servers. The JTAV Technical Support Center will grant specific exceptions to this in writing.

g. Equipment and media which has been used in conjunction with the SECRET JTAV Server will be sanitized or destroyed in accordance with applicable DOD and local regulations.

h. Problems, violations or deviations from these procedures must be reported to the JTAV Support Office – Pacific at (808) 477-4223 or via e-mail to jtavhelp@hq.pacom.mil. Written correspondence should be addressed to USCINCPAC, JTAV Support Office – Pacific, PO Box 64020, Camp H.M Smith, HI 96861-4020.

3. USERID and PASSWORD.

a. Each JTAV user is personally responsible for protecting and properly using the LAN userid and password issued to the user.

b. There will be no group accounts permitted on any JTAV Server.

c. Unclassified JTAV Server User IDs are UNCLASSIFIED. Unclassified JTAV Server passwords are UNCLASSIFIED SENSITIVE.

d. Secret JTAV Server User IDs are UNCLASSIFIED. Secret JTAV Server passwords are SECRET.

e. JTAV User IDs and Passwords are individual identifiers. The purpose of these is to control access and to establish accountability for use of JTAV resources. Users SHALL NOT: (1) Use any means other than their assigned User IDs and passwords to access the servers; (2) Divulge their passwords to any other person(s); (3) surrender physical control of a JTAV Session without first logging off; or (4) allow third parties the use their account.

4. LABELING and RELEASE OF OUTPUT DATA.

a. The JTAV Servers cannot be trusted to separate or identify data by security classification, nor to apply security markings to output on hardcopy, monitors or computer media.

b. All hardcopy output shall be protected at the appropriate level: (1) JTAV
Unclassified Server data will be treated as For Official Use Only - FOUO; or
(2) JTAV Secret Server data will be treated as SECRET.

c. All removable computer storage media, to include unclassified media that is associated with JTAV data must be labeled with security markings. These labels are essential for positive identification of classified media, and to prevent unintentional contamination of unclassified media with classified data.

d. Users who create classified e-mail shall properly mark the header and the body of said e-mails to reflect the classification of the message.

e. All equipment or storage media, which has been used to store, display or access the JTAV Servers, shall be marked according to the data it handles.

5. COMPUTER VIRUSES.

a. Upon detection of a computer virus, JTAV Server account holders shall notify the JTAV Support Office – Pacific immediately.

6. STATEMENT OF UNDERSTANDING.

a. I acknowledge having read this Security Briefing, and shall comply with all its provisions.

b. I understand that a violation of these provisions may result in: (1) a degradation of the operational readiness of this command; (2) the compromise of classified information; (3) the criminal prosecution under the Uniform Code of Military Justice and/or the United States Code; (4) administrative action to include termination of employment; and (5) revocation of JTAV server access.

SIGNATURE _________________________ DATE _10/10/2000___

PRINTED NAME & RANK __________________ GRADE _____________

ORGANIZATION ________________________ PCS DATE___________

Ver. 10/97

DRAFT

APPENDIX G

JTAV IT HELP DESK PROCEDURES

1. Hours of Operations. Standard Hours of Operation for the JTAV IT Support Office – Pacific (JSOP) are Monday through Friday 7:30 a.m. to 4:30 p.m. Hawaii Standard Time (HST). During times of special operations, the JSOP will support operations as directed by USCINPAC J4

2. JTAV Trouble Calls.

   a. The JSOP Help Desk Coordinator (HDC) should be seen as the first contact for any issues regarding either of the JTAV IT applications (i.e., Client/ Server or Web). If a user is unsure of the cause of a problem, do not hesitate to call JSOP HDC for any assistance. Any functional questions may also be addressed to the JSOP HDC. The best way to reach us is via email.

3. System Discrepancy Report. Should operating problems be encountered with either the JTAV IT "Client/Server" desktop application or using the JTAV IT Web capability , the user should open up a System Discrepancy Report (SDR) and fill out pertinent information. Upon completion, the SDR needs to be saved in text format and attached as an email to the JSOP Help Desk at jtavhelp@hq.pacom.mil. If unable to email for any technical reason, please fax a copy to the Help Desk at (808) 477-0921. The SDR is the prime mode of tracking trouble calls and discrepancies. SDRs that are generated electronically through JTAV IT capability are able to be tracked through the JTAV "resolution process" by the user.

   a. To generate an SDR in the "client/server" mode, do the following:

      Once in the application, go to the **Help** pull down menu;
      Click on SDR;
      Fill in the form with appropriate information;
      Click Save, make sure that you save as text (.txt); and
      Compose an email and attach the text and send it to jtavhelp@hq.pacom.mil

   b. To generate an SDR in the "Web" mode, do the following:
      Click on "Comments";
      Type a description of the problem and address the severity of the problem, and;
      Hit "Send" and it will go automatically to USPACOM.

4. System Change Requests. The System Change Request (SCR) provides a way for you to identify desired changes to the JTAV system capability. (Note: Use the SDR for system technical problems, only). To access the form, follow the outline below.

   a. To generate an SCR in the "Client/Server"mode, do the following:
      Once in the application, go to the **Help** pull down menu;
      Click on "SCR";
Fill in the form with appropriate information;
      Click "Save"; make sure that you save as text (.txt); and,
      Compose an email and attach the text and send it to jtavhelp@hq.pacom.mil.

b. To generate an SCR in the Web mode, follow the directions listed for generating an SDR on the Web in paragraph 3.b. above.

5. Users are also able to reach the JSOP Help Desk Coordinator by calling (808) 477-4223. Should the JSOP Help Desk Coordinator not be available, leave a message on the answering machine. Upon retrieving the message the Help Desk will contact the user.